UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,513	07/08/2003	R. Bruce Wallace	15929ROUS02U	9214

34645 7590 08/31/2009

Anderson Gorecki & Manaras, LLP
Attn: John C. Gorecki
P.O BOX 553
CARLISLE, MA 01741

EXAMINER	
PATEL, NIRAV B	
ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
08/31/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

john@gorecki.us
jgorecki@smmalaw.com
officeadmin@smmalaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/615,513
Filing Date: July 08, 2003
Appellant(s): WALLACE ET AL.

John C. Gorecki (Reg. No. 38,471)

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed June 08, 2009 appealing from the Office action mailed Oct. 23, 2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments

The appellant's statement of the status of amendments contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Hamilton (US Patent No. 7,123,974 – Nov. 19, 2002)

Daniely (US Patent No. 6,763,469 – Feb. 17, 2000)

Danner et al. (US Patent No. 7,194,003 – Jan 31, 2002)

Schmitz et al. (US Patent No. 6,172,430 – Dec. 16, 1998)

Amara et al. (US Pub. No. 2004/0083295 – Oct 24, 2002)

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-3, 7, 9-11, 13-15 and 17, 18, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton (US Patent No. 7,123,974) and in view of Daniely (US Pub. No. 6,763,469).

As per claim 1, Hamilton teaches:

a local area network; one or more programmable logic controller [Fig. 1]; and a security policy implementation point (SPIP) connected between the network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the network [Fig. 1, 2, 6], the SPIP

being configured participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network [Fig. 6, col. 9 lines 7-33].

Hamilton teaches the SPIP connected between the network and the one or more programmable logic controllers [Fig. 1, 6], to prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP and authorized to take action on the one or more programmable logic controllers isolated by the SPIP [col. 9 lines 7-12, col. 10 lines 45-60, Fig. 2, 3, 6 - associated text].

Daniely teaches: a security policy implementation point (security device) connected between the local area network and the one or more component (device) to isolate the device from the local area network to prevent a person using a management program from accessing the one ore more devices over the local area network unless authenticated to the SPIP and authorized to take action on the SPIP, the SPIP being configured to participate in a Virtual Private Network (VPN) such that communications between the management program and the SPIP over the industrial network occur over a VPN tunnel [Fig. 1A, 1B, col. 5 lines 1-10, 51-65, col. 6 lines 24-47].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Daniely with Hamilton, since one would have been motivated to provide flexible network security at the local level, which provides protection for computer/device against unauthorized access and permit authorized access within an organization [Daniely, col. 2 lines 42-44, col. 1 lines 60-63].

As per claim 2, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP, the programmable logic controller [Fig. 1, 6] and wherein the SPIP is logically connected between the network and the one or more programmable logic controllers [Fig. 1, 6].
Daniely teaches the SPIP (security policy/rules) is integrated with the programmable logic controllers (devices – e.g. computers, switches, routers, servers, gateways, devices) [Fig. 1A, 1B] and wherein the SPIP is logically connected between the local area network and the one or more devices/components [Fig. 1A].

As per claim 3, the rejection of claim 1 is incorporated and Hamilton teaches the network contains a plurality of programmable logic controller [Fig. 1], wherein the one or more programmable logic controller are subset of the plurality of programmable logic controllers [Fig. 1, 2] and wherein the SPIP is physically disposed between the network and the one or more programmable logic controllers [Fig. 1].
Daniely teaches the SPIP is physically connected between the local area network and the one or more devices/components [Fig. 1A].

As per claim 7, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP is further configured to apply policy to limit access to the programmable logic controllers to individuals authorized to access the programmable logic controllers and to require authentication on the SPIP before allowing control instructions to pass from the local area network through the SPIP to the one or more programmable logic controller [Fig.1, 6, col. 9 lines 7-33].

As per claim 9, the rejection of claim 1 is incorporated and Hamilton teaches the industrial network is an untrusted network configured to interconnect network services with a plurality of SPIPs associated with factory machines, and wherein the network services are configured to enable operation of the factory machines to be altered through the industrial network [Fig. 1, 2, 6, col. 9 lines 7-33].

As per claim 10, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP is further configured to enable local access to the one or more programmable logic controllers by applying a local authentication and authorization policy, to enable the SPIP to enforce network policy in connection with attempted local access [Fig. 1, 6, col. 9 lines 7-33].

As per claim 11, the rejection of claim 10 is incorporated and Hamilton teaches a local access policy configured to require authentication and authorization of at least one of an user and an. accessing electronic device for non-emergency attempts to access the SPIP, and an alternate access policy configured to allow access to the SPIP and maintain an audit log attendant to a local attempt to access the SPIP [Fig. 1, 6, col. 9 lines 7-33].

As per claim 13, the rejection of claim 11 is incorporated and Hamilton teaches the SPIP comprises a local authentication policy and information associated with authorized

users and indicative of authorization policy information associated with said at least one factory machine [Fig. 1, 6, col. 9 lines 7-33].

Daniely teaches the local authentication policy and information associated with authorized users and devices [col. 5 lines 1-9, 50-63, col. 6 lines 24-41].

As per claim 14, Hamilton teaches:

a local path configured to implement a local access policy related to direct local access to one or more programmable logic controllers [Fig.1, 2, 6, col. 9 lines 7-33]; and a network path connected between the industrial network and the one or more programmable logic controllers to control access to the programmable logic controller via the industrial network [Fig. 1, 2, 6, col. 9 lines 7-33], the network path being configured to isolate the one or more programmable logic controllers and associated factory machines from the industrial network by participation in a Virtual Private Network such that communications with the SPIP over the industrial network utilize the Virtual Private Networks [Fig. 1, 2, 6, col. 9 lines 7-33]. Hamilton teaches the SPIP connected between the network and the one or more programmable logic controllers [Fig. 1, 6], to prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP and authorized to take action on the one or more programmable logic controllers protected by the SPIP [col. 9 lines 7-12, col. 10 lines 45-60, Fig. 2, 3, 6 - associated text].

Daniely teaches: a security policy implementation point (security device) connected between the local area network and the one or more component (device) to isolate the device from the local area network to prevent a person using a management program from accessing the one ore more devices over the local area network unless authenticated to the SPIP and authorized to take action on the SPIP, the SPIP being configured to participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network occur over a VPN tunnel [Fig. 1A, 1B, col. 5 lines 1-10, 51-65, col. 6 lines 24-47].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Daniely with Hamilton, since one would have been motivated to provide flexible network security at the local level, which provides protection for computer/device against unauthorized access and permit authorized access within an organization [Daniely, col. 2 lines 42-44, col. 1 lines 60-63].

As per claim 15, the rejection of claim 14 is incorporated and Hamilton teaches programmable logic controller circuitry configured to implement the one or more programmable logic controllers and to function to control at least one factory machine [Fig. 1, 2].

As per claim 17, the rejection of claim 16 is incorporated and Hamilton teaches the local path further comprises an accounting module configured to record accesses to at least

one of the SPIP, an associated programmable logic controller, and an associated factory machine [Fig. 1, 4, 5, 7].

As per claim 18, the rejection of claim 15 is incorporated and Hamilton teaches the local path comprises an authentication module configured to authenticate the identity of an individual seeking to access a device through the SPIP, and an authorization module configured to assess an authorization associated with the individual to ascertain whether the individual is authorized to access the device [Fig. 1, 6, col. 9 lines 7-33].

As per claim 21, the rejection of claim 15 is incorporated and Hamilton teaches the SPIP is configured to apply policy to limit access to the programmable logic controllers to individuals authorized to access the programmable logic controllers and to require authentication on the SPIP before allowing control instructions to pass from the industrial network through the SPIP to the one or more programmable logic controllers [Fig. 1, 2, 6, col. 9 lines 7-33].

As per claim 22, the rejection of claim 15 is incorporated and Hamilton teaches network ports configured to interface with the industrial network, and output ports configured to interface with a programmable logic controller [Fig. 1, 2].

2. Claims 4-6 and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton (US Patent No. 7,123,974) in view of Daniely (US Pub. No. 6,763,469) and in view of Danner et al (US Patent No. 7,194,003).

As per claim 4, the rejection of claim 3 is incorporated and Hamilton teaches the local area network is an Ethernet network, wherein the SPITP is configured to communicate with network devices on the local area network over the Ethernet network [Fig. 1, 2, col. 5 lines 55-60].

Danner teaches the switch is configured to communicate with the programmable logic controller using a protocol selected from at least one of Profibus, Controller Area Network, RS-232, RS-422, and RS-485 [col. 7 lines 1-9].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Danner with Hamilton and Daniely, since one would have been motivated to provide flexible network security at the local level [Daniely, col. 2 lines 43-44].

As per claim 5, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP is included as blade in the network device [Fig. 6].

Danner teaches the local area network includes at least one Ethernet switch/router [Fig. 3].

As per claim 6, the rejection of claim 1 is incorporated and Hamilton teaches the SPIP is configured to implement security policy to control network access to at least one PLC through the SPIP [Fig. 1, 6, col. 9 lines 7-33]. Danner teaches at least one PLC connected to the Ethernet switch/router [Fig. 3].

As per claim 23, the rejection of claim 22 is incorporated and Hamilton teaches communication with the industrial control components and with remote devices as shown in Fig. 1, 2.
Danner teaches communicate on the industrial network utilizing an Ethernet protocol [col. 7 lines 17-39] and communicate with the programmable logic controller using a protocol understandable by the programmable logic controller [col. 7 lines 1-9].

As per claim 24, the rejection of claim 15 is incorporated and Danner teaches network ports configured to interface with the industrial network, control logic configured to implement a control program associated with a programmable logic controller, and interface ports configured to interface with a factory machine [Fig. 3, col. 6 lines 4-47].

As per claim 25, the rejection of claim 24 is incorporated and Danner teaches the interface ports comprise at least one input port configured to receive input from an environmental sensor, and at least one output port configured to control at least one electro-mechanical device [Fig. 3, col. 6 lines 4-47, 60-67, col. 7 lines 10-39].

3. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton (US Patent No. 7,123,974) in view of Daniely (US Pub. No. 6,763,469) and in view of Schmitz et al (US Patent No. 6,172,430).

As per claim 16, the rejection of claim 15 is incorporated and Hamilton teaches the local access policy for enabling access to the factory machine based on the authentication and authorization process associated with a user [col. 9 lines 7-24]. Hamilton doesn't expressively mention to enable operation of the factory machine to be altered without verification of authorization and authentication of a user during an emergency.
Schmitz teaches: enable operation of the factory machine to be altered without verification of authorization and authentication of a user during an emergency [col. 5 lines 7-10].
Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Schmitz with Hamilton and Daniely, since one would have been motivated to prevent the hazardous condition.

4. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton (US Patent No. 7,123,974) in view of Daniely (US Pub. No. 6,763,469) and in view of Amara et al (US Pub. No. 2004/0083295).

As per claim 19, the rejection of claim 18 is incorporated and Hamilton teaches the authentication module and the authorization module [col. 9 lines 17-24].

Amara teaches interface to a Remote Access Dial In User Service (RADIUS) server [paragraph 0040]. Further, Amara teaches authentication and authorization mechanism utilize *other remote access software product* (e.g. RADIUS, DIAMETER, LDAP, etc.) [paragraph 0040, 0042].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Amara with Hamilton, since one would have been motivated to provide scalable network access system [Amara, paragraph 0006, 0007].

As per claim 20, the rejection of claim 18 is incorporated and Hamilton teaches the authentication and authorization modules maintain a local copy of authorized users and authentication policy to allow local access to the SPIP [col. 9 lines 24-29].

Amara teaches maintain a local copy of authorized users and authentication policy [paragraph 0046, 0047, 0027].

(10) Response to Argument

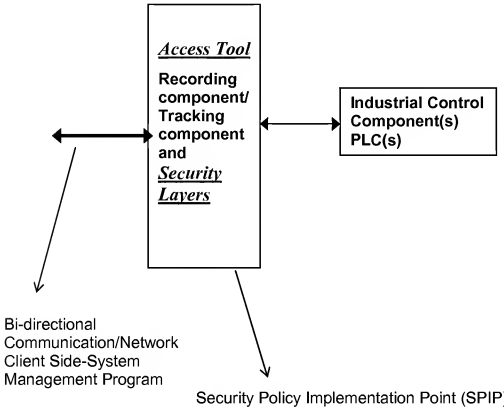
Appellant's arguments filed on June 08, 2009 have been fully considered but they are not persuasive.

Independent claim 1, and dependent claims 2-3, 7, 9-11 and 13

Regarding to appellant's argument, Examiner disagrees with Appellant since Hamilton's invention relates to a system and methodology to provide electronic audit recording and

tracking of interactions with an industrial control system in order to facilitate access to such systems in a controlled manner. When application (management program - client side) logs on or communicates to a respective control system component, the recording component records all interactions with the control system during a current session (e.g. access dates, access times, user names, type of access...etc.). The access tool (20) includes any type of hardware and/or software (e.g. editing tool, programming tool, communications component, monitoring component) that interact with the industrial control components 24, which includes programmable logic controllers (PLCs) [Fig. 1, col. 4 lines 57-66], wherein the network (30) includes local factory networks and/or public network. An access tool (recording & tracking components and *security layers*) interacts with one or more industrial control components via a network. The client system includes at least one application (the management program) that interacts with a client communications component to exchange data with the controller (the industrial control system) over the network. The access tool is provided to monitor the interaction over the network and also performed authentication procedure to provide authorized access [col. 6 lines 43-48]. Further, the access tool comprises one ore more security layers such as encryption techniques, authentication and/or authorization techniques and/or other security measures when communicating activity data over the network, virtual private networks...etc. [col. 9 lines 7-33, Fig. 6]. The security layers include one ore more trust components to provide user authentication, authorization, a policy component to facilitate varying levels of access. Therefore, the application (on the client system/side) is a management program that accesses the one ore more controllers

(programmable logic controllers) over the network and the access tool is a security policy implementation point (SPIP) that protects the one ore more controllers (programmable logic controllers) from unauthorized access as claimed.



Further, Daniely's invention relates to a system and method for providing local network security for each computer connected to the network, which would provide individual protection for each computer (e.g. PLC) against unauthorized access. A security agent 18 controls two sets of rules for providing security to each computer in the network. The first set of rules is the list of declaration according to which packets are filtered by local security device. The second set of rules is the list of access permissions for each user wishing to gain access to any part of organizational network. Once security agent has

authenticated the user, the security agent then determines privileges for the user. Therefore, Daniely's invention provides precision and flexibility for determining security of network, as well as protecting both virtual networks and physical network. In this case, the combination of Hamilton and Daniely teaches the claim subject matter and the combination is sufficient to incorporate the teaching of Daniely into the teaching of Hamilton. The modification would be obvious because one of ordinary skill in the art would be motivated to provide flexible network security at the local level, which provides protection for computer/device against unauthorized access and permit authorized access within an organization. Furthermore, the examiner recognizes that obviousness can also be established by combining or modifying the teaching of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to on of ordinary skill in the art. See *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ 2nd 1941 (Fed. Cir 1992).

Independent claim 14, and dependent claims 15-25

Regarding to appellant's argument, Examiner disagrees with Appellant since Hamilton teaches the network path (via access tool) as above, connected between the industrial network and the one or more programmable logic controllers to control access to the programmable logic controller via the network and prevent a person using a

management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP and authorized to take action on the one or more programmable logic controllers protected by the SPIP.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Nirav Patel /
Examiner, Art Unit 2435

Conferees:

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435

/Beemnet W Dada/
Primary Examiner, Art Unit 2435